REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

By this Amendment, Claims 19, 33 and 39 have been amended to more clearly recite subject matter Applicants regard as their invention, as discussed in detail below. Claim 19 has also been amended to include subject matter of Claims 20 and 22, which are now canceled without prejudice or disclaimer. Claims 21, 23, 25-29 and 34-36 have also been amended for consistency. Claim 40 has been canceled without prejudice or disclaimer to reduce the issues. Claims 1-18 and 37-38 were previously canceled without prejudice or disclaimer. Thus, Claims 19, 21, 23-36 and 39 are pending.

In the Office Action, Claims 19-36 and 39-40 were rejected under 35 U.S.C. § 103(a) over David Chaum et al., "Group Signatures", XP-000900793 ("Chaum") in combination with Saito.

Without acceding to the rejection, Claim 19 now recites, *inter alia*, signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C); and means for outputting the message (m) and the group signature (S) to a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that the message (m) is associated with the group (G) based on the group signature (S), with the identity of the member (M) of the group (G) remaining anonymous to the checker. Support is provided, for example, at page 1, lines 10-18; page 7, lines 6-17; and page 22, lines 4-6, of Applicants' disclosure. It is

apparent that the applied references do not teach or suggest at least the above combination of features.

For example, Chaum teaches four group signature schemes that allow for anonymity of the member of the group who signed the message. *See* Chaum, page 1, Abstract. However, in contrast with the subject matter recited in Claim 19, in each of Chaum's group signature schemes the group signature is understood as being produced by a member, *i*, of the group by using a secret signing key that is specific to the member *i* who signs the message. *See* Chaum, page 259 ("s_i" or "$s_i r_i$" for the first scheme); page 259 ("s_i" for the second scheme); pages 262-263 ("p_i" for the third scheme); and page 263 ("s_i" for the fourth scheme). Chaum therefore teaches and suggests that group signature schemes require using a specific signature key for each group member, in contrast with the subject matter of Claim 19. Thus, none of Chaum's group signature schemes are understood as teaching or suggesting, as a minimum, signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members, as recited in Claim 19.

Furthermore, Claim 19 also recites, *inter alia*, encryption means (B3) for producing an encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz); and signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C). Thus, Claim 19 is directed to encryption means (B3) for producing an encrypted text (C), and distinct signing means (B6) for producing the group signature (S). The applied references are not understood as teaching or suggesting the above combination of features.

For example, contrary to the allegations contained in the final Office Action (for example, item 11 of the Office Action), the cited portion of Chaum discussing the uses of the "same secret key" is not understood as teaching or suggesting encryption means (B3) for producing an encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz); and signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C), as recited in Claim 19.

Secondary reference Saito is not understood to remedy the above-discussed deficiencies of Chaum. For example, Saito teaches a data verifying apparatus and method in which a message is accompanied by a digital signature using a private key associated with a particular person. *See* Saito, col. 7, lines 35-42 and 52-53; and col. 11, lines 46-49 ("token private key"). Saito does not appear to teach or suggest signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C); and means for outputting the message (m) and the group signature (S) to a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that the message (m) is associated with the group (G) based on the group signature (S), with the identity of the member (M) of the group (G) remaining anonymous to the checker, as recited in Claim 19.

Therefore, Applicants respectfully submit that Claim 19 distinguishes patentably from the applied references.

Independent Claim 33 recites, *inter alia*, a method for secure communication of message (m) sent by a member (M) of a group (G) using a group signature (S), the

method comprising producing the group signature (S) of the message (m) by signing, with a private signature key (SK) common to all group members, a set including the message (m) and encrypted text (C) produced by using a personalized data (Z, Kz).

In addition, independent Claim 39 recites, *inter alia*, a group signature system for ensuring a secure communication of a message (m) sent by a member (M) of a group (G) using a group signature (S), including an electronic device configured to store a personalized data (z, Kz) identifying the member (M) of the group (G), to produce an encrypted text (C) intended to be associated with said message (m) using said personalized data (z, Kz), and to produce the group signature (S) with a private signature key (SK) common to all group members using the message (m) and said encrypted text (C), and to output the message (m) and the group signature (S); and a checker that receives the message (m) accompanied by the group signature (S) output from the electronic device, the checker being configured to verify that the message (m) is associated with the group (G) based on the group signature (S), the identity of the member (M) remaining anonymous to the checker.

Therefore, Applicants respectfully submit that Claims 33 and 39 also distinguish patentably from the applied references for at least the reasons discussed above with respect to Claim 19.

The remaining Claims 21, 23-32 and 34-36 are also believed to distinguish patentably due to their respective dependence from Claims 19 and 33, as well as for the additional features recited in Claims 21, 23-32 and 34-36.

Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully requested.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2678-9156US01) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

Date: February 26, 2008

By: /Eric G. King/
Edward J. Kondracki
Reg. No. 20,604

Eric G. King
Reg. No. 42,736

Miles & Stockbridge, P.C.
1751 Pinnacle Drive
Suite 500
McLean, Virginia 22102-3833
(703) 610-8647
4851-0148-9410